Robinson+Cole

The New York Cybersecurity Regulation: What This Means To You And Your Organization

FEBRUARY 27, 2017

Agenda

- *The Significance* of the New York Department of Financial Services Cybersecurity Regulation
- *The Evolution* of the Regulation
- *The Challenges* presented by the Regulation
- *The Impact* of the Regulation on the C-Suite
- *The Plan*: Compliance and Beyond

The Cybersecurity Backdrop

- **Cyber crime costs $400 billion annually – Lloyd's**
- **Global cyber insurance uptake growing 21% annually**
  - $2.5 billion in written cyber premiums in 2016
- **Rating agencies now addressing cyber-maturity in credit ratings**
- **Cybersecurity is dominant risk for CEOs**
  - 70% view it a major threat
  - $3 trillion market value destroyed in 2015
  - "Top 5" risk likelihood – 2017 World Economic Forum
- **Most companies remain unprepared:**
  - Only 58% of companies have resources to comply with security regulations
  - 1.5 million InfoSec job shortage by 2019
  - Only 21% of companies at "mature" stage
  - Only 1/3 of corporations have a data breach response plan

The Significance

- Billed as a “first-in-the-nation” regulation concerning cybersecurity
- Arguably the most stringent broadly applicable cyber regulation in existence
- Goes beyond other data privacy and cybersecurity regulations, including the Graham Leach Bliley Act
- Covers information and systems that do not include, store, process or maintain PII
- Requires new compliance processes and is built around the Risk Assessment
- Likely modification and expansion of existing protocols to meet regulatory requirements
- C-Suite must personally certify compliance with the Regulation on an annual basis

The Evolution

- Over the past several years, DFS has surveyed close to 200 regulated banking institutions and insurance companies and has met with cybersecurity experts
- Based on that feedback, DFS issued a proposed regulation on September 13, 2016
- DFS received over 150 public comments
- DFS considered those comments and issued a revised proposed regulation on December 28, 2016
- On February 16, 2017, DFS released the final versions of the Regulation, making only minor technical changes

Key Dates & Brass Tacks

- **Applies to financial services companies licensed to do business in NY**

- **March 1, 2017 –**Effective Date
- **September 1, 2017 –**Compliance with many provision of the regulations expectation by DFS
- **February 15, 2018 –** Initial Certification of Compliance
- **Transitional Periods:**
  - **March 1, 2018** – "Baseline" reports, assessments, capabilities, activities
  - **September 1, 2018** – Advanced capabilities in place
  - **March 1, 2019** – Third Party Service Provider Security Policy implemented

Policies & Procedures

- Risk Assessment (Basis for other policies and procedures/actions)
- Written Cybersecurity Policy
- 3rd Party Information Security Policy
- Limitations on Data Retention
- Training & Monitoring
- Incident & Response Plan
- Application Security

Required Actions

- Establishment of Qualified Chief Information Security Officer (“CISO”)
- Penetration Testing
  Vulnerability Assessments
  Encryption of Data at Rest and in Transit
- Preservation of Audit Data (to reconstruct transactions and cyber events)
- Data Minimization
- Notices to Superintendent

Assessments & Reports

- CISO Assessment
- Risk Assessment (outcome used to develop policies and procedures)
- Annual Statement of Compliance (by named C-Suite or Chairman of the Board)
- Notice of material Cybersecurity Event (within 72 hours)

The Challenges

- Cybersecurity program
- Cybersecurity policy
- Risk Assessment
- Chief Information Security Officer
- Audits/logs
- Encryption and SDLC (secure software development lifecycle)
- Reporting Requirements
- Third-party Service Providers

Cybersecurity Program

- Each company “shall establish and maintain a cybersecurity program designed to ensure the confidentiality, integrity and availability of the Covered Entity’s Information Systems.”

- The cybersecurity program shall be based on the Covered Entity’s Risk Assessment and designed to perform core cybersecurity functions

Cybersecurity Policy

- The written cybersecurity policy mandated by the Regulation must be approved by a “Senior Officer” and is detailed, requiring inclusion of 14 key areas, many of which are found in traditional information security policies and procedures, but also include others such as customer data privacy, business continuity, vendor and third-party service provider management, and incident response

- Based on the responsibilities outlined in the Regulation, the “Senior Officer” is effectively the CEO or a committee of senior management, operations, technology, security, compliance and risk officers

- The policy must be based on the Risk Assessment

Risk Assessment

- Risk Assessment is the backbone of the cybersecurity program
- Must be carried out in accordance with written policies and procedures and must be documented in writing
- policies and procedures shall include:
  - (1) criteria for the evaluation and categorization of identified risks or threats facing the Covered Entity;
  - (2) criteria for the assessment of the confidentiality, integrity and availability of the Covered Entity's Information Systems, including the adequacy of existing controls *in the context of identified risks*; and
  - (3) requirements describing how identified risks will be mitigated or accepted based on the Risk Assessment and how the cybersecurity program will address the risks.

Chief Information Security Officer

- Covered Entities will have to designate a “qualified individual” to serve as the CISO who will be “responsible for overseeing and implementing the [company’s] cybersecurity program and enforcing its cybersecurity policy.”

- Covered Entities must have cybersecurity personnel sufficient to manage the cybersecurity risks and perform the core functions

- The CISO will be responsible for producing report at least annually

Third Party Service Providers

- The Regulation seeks to manage the risk from third-party service provider relationships by setting out policies and procedures that address:
  - A risk identification and assessment of the third-party
  - Minimum cybersecurity practices required to be met by the third-party in order for them to do business with the Covered Entity
  - A due diligence process to evaluate the third-party's cybersecurity programs
  - Periodic assessment of the adequacy of the third-party's cybersecurity practices
  - Policy must include relevant guidelines for due diligence and/or contractual protections, including, as applicable:
    - Multi-factor authentication
    - Encryption of data in transit and at rest
    - Prompt notice of Cybersecurity Events
    - Identification of protection services for customers affected by third-party's negligence or willful misconduct
    - Representations and warranties re: cybersecurity policies and procedures
    - Right to perform cybersecurity audits

Incident Response Plan and Notice

- As part of the cybersecurity program, the Covered Entity must establish an incidence response plan to respond to or recover from a cybersecurity breach or attempted breach

- Notice to the Superintendent within 72 hours from a determination that a Cybersecurity Event has occurred and has "a reasonable likelihood of **materially harming** any **material part of the normal operation(s)** of the Covered Entity"
  - Determinations of materiality may impact public filing requirements

Annual Compliance Certification

- The Regulation requires a Covered Entity to submit to DFS a written Certification of Compliance by February 15, 2018

- The written statement would require the signature of the Chairperson of the Board of Directors of the entity or **named** Senior Officer(s) (i.e. CEO or committee) certifying that such person has reviewed documents, reports, certifications and opinions of such officers, employees, representatives and outside vendors

- Similar to a Sarbanes-Oxley 404 certification

The Impact

- Elevates cybersecurity to the C-Suite
- Forces companies take a hard look at their practices and tailor their program accordingly
- Allows for flexibility in risk mitigation planning but places the onus on company
- Charters course for future regulations

The Plan

- Dust off the old cybersecurity policies
- Identify the right team
- Start with the Risk Assessment policy
- Search for or appoint a CISO
- Work with third-party service providers to ensure compliance
- Consult with your lawyers and technical consultants

Questions

RICHARD M. BORDEN
rborden@rc.com

Robinson & Cole LLP
280 Trumbull Street
Hartford, CT 06103

ANDREA DONOVAN NAPP
anapp@rc.com

Robinson & Cole LLP
280 Trumbull Street
Hartford, CT 06103

LINN F. FREEDMAN
lfreedman@rc.com

Robinson & Cole LLP
One Financial Plaza
Suite 1430
Providence, RI 02903